

Promoting the availability of secure telecommunications networks



DESCRIPTION

Date of publication

4 June 2009

Authors (from body; name, chairman and secretary of the body) Working group on Promoting the availability of secure telecommunications networks; Chair: Matti Lehti, Helsinki School of Economics HSE; Vice-Chair: Harri Pursiainen, Ministry of Transport and Communications; Secretaries: Juhapekka Ristola and Rauli Parmes, Ministry of Transport and Communications		Type of publication Report	
		Assigned by Suvi Lindén, Minister of Communications	
		Date when body appointed 15 January 2009	
Name of the publication Promoting the availability of secure telecommunications networks			
Abstract <p>It was necessary to take a view concerning the protection of advanced critical infrastructure under exceptional circumstances and also during serious disruptive situations in normal circumstances, on account of the following factors: society has become more information-intensive; foreign ownership has increased; functions are outsourced; ICT systems are more integrated and interdependent; usage of freely accessible information networks; and the greater dependence on electricity.</p> <p>With due consideration to the aims of the work and having assessed the current state and development needs, the working group decided unanimously to propose that among others the following measures be taken</p> <ul style="list-style-type: none">- Under the direction of the Government's ownership steering department, it should be ensured that the state always has sufficient ownership and control authority concerning at least those elements of the fixed telecommunications networks most critical to the functioning of society. This objective should be implemented in such a way that, to guarantee security, the amount of the state's capital tied up in the ownership of telecommunications companies is as little as possible, and that the actions needed are targeted in such a way that there is no justified cause to assume that they will hinder the pursuit of a communications policy that is independent of state ownership.- The Ministry of Transport and Communications should set up a standing committee of public servants, composed of representatives of the main ministries and other authorities, for the purpose of supporting and coordinating official tasks concerning the regulation of communications markets, the availability of electronic networks for public authorities, and the ownership policy with regard to communications companies.- In implementing the proposals, the high security national information infrastructure produced by the security network project for the government sector should be utilised wherever possible.			
Keywords security of supply, security of operations, networks, ownership of telecommunications operators			
Miscellaneous Contact persons: Matti Lehti, Chancellor and Harri Pursiainen Permanent Secretary of the Ministry of Transport and Communications			
Serial name and number Publications of the Ministry of Transport and Communications 28/2009		ISSN 1457-7488 (printed version) 1795-4045 (electronic version)	ISBN 978-952-243-067-0 (printed version) 978-952-243-068-7 (electronic version)
Pages, total (printed version) 38	Language English	Price	Confidence status Public
Distributed and published by Ministry of Transport and Communications			

CONTENTS

1 OVERVIEW	3
1.1 Working group	3
1.2 Summary	6
2 AIMS.....	9
2.1 Importance of secure communications networks.....	9
2.2 Communications policy objectives	10
2.3 Parties involved and operating methods	11
2.4 Critical operating processes in Finland's information society.....	14
3 Current state and development needs.....	16
3.1 Current state	16
3.1.1 Availability of communications networks and services	16
3.1.2 Changes occurring in communications networks and markets.....	19
3.1.3 Legislation.....	22
3.1.4 International comparison.....	22
3.1.5 Government investment in the ICT sector	24
3.2 Development needs.....	25
3.2.1 Identifying parties that are critical for the security of supply	25
3.2.2 Cooperation.....	25
3.2.3 Utilising market mechanisms.....	26
3.2.4 Legislation.....	26
3.2.5 State ownership in the communications market	28
4 PROPOSED DEVELOPMENT MEASURES AND THEIR EFFECTS IN BRIEF.....	29

1 OVERVIEW

1.1 Working group

Background

ICT systems that are secure and meet the requirements concerning Finland's security of supply are an essential prerequisite for businesses, government and the everyday transactions of citizens in Finland's information society. The importance of ICT systems was emphasized in the 2004 Government report on Finnish security and defence policy, in the Government resolution on the strategy for securing the functions vital to society, issued in November 2006, and in the Government decision on safeguarding the security of supply, issued in August 2008. Securing ICT systems in accordance with these decisions has required, and will continue to require, communications policy actions, steps by the Government and by businesses to ensure the security of supply, and actions by public authorities, especially those responsible for security, to secure their own critical systems.

Establishment of working group

On 15 January 2009, the Ministry of Transport and Communications established a working group to examine the means by which the availability of telecommunications networks that are secure and meet the requirements for security of supply can be promoted on the communications market. The working group's term ended on 15 May 2009.

The aim of the working group was to create a basis and alternative models for communications policy actions and other Government actions for promoting the availability of telecommunications networks and telecommunications services on the market, such that this would meet the need more effectively than at present for securing the functions vital to society, and especially to government, and for Finland's security of supply. The working group was required to draft a description of the current state of affairs and of the envisioned future state. On the basis of this, the working group was also required to present proposals for alternative ways of achieving the envisioned future state and to evaluate the effects of these alternatives. The report had to include estimates of the financial and legislative implications of the measures and of their significance for economic growth and for developing innovations.

Composition of working group

Matti Lehti, Chancellor of the Helsinki School of Economics, was invited to be the working group's chairman, and *Harri Pursiainen*, Permanent Secretary at the Ministry of Transport and Communications, was designated vice chairman.

The following were invited to be members of the working group: *Risto Volanen*, State Secretary at the Prime Minister's Office, *Raimo Luoma*, Director General at the Ministry of Employment and the Economy, *Pekka Timonen*, Director General of the Ownership Steering Department at the Prime Minister's Office, *Rauni Hagman*, Director General of the Finnish Communications Regulatory Authority, and *Ilkka Kananen*, Managing Director of the National Emergency Supply Agency. *Juhani Jokinen*, Director General of the Finnish Competition Authority, was invited to be a permanent advisor, and he was given the opportunity to designate a deputy from the Finnish Competition Authority as necessary.

Juhapekka Ristola, Director of the Communications Networks Unit, and *Rauli Parmes*, Director of Security and Office Services, both at the Ministry of Transport and Communications, were designated as secretaries for the working group.

The working group consulted the ministries that represent the authorities in charge of security and also, to the extent required by the scope of their remit, other public authorities, companies in the sector and other bodies.

Concepts used by the working group and public access to its report

Most of the working group's report is public information. However, its detailed appendices are confidential on the basis of paragraphs 7, 8 and 20 of section 24 of the Act on the Openness of Government Activities. The working group has, for the most part, followed the established concepts used in the ICT sector. It has nevertheless used the terms communications network and telecommunications network to refer to the same concept, the choice of term depending on the context or the established usage. Similarly, when describing requirements, the concepts of secure network, secure system and meeting security of supply requirements have been used somewhat interchangeably.

The working group was given the task of reporting on the means by which the availability of telecommunications networks that are secure and meet the requirements for security of supply can be promoted on the communications market. .

Note on assessment of effects and international comparison

In drawing up its report, the working group observed that any detailed analysis, particularly of the effects of various ownership policy alternatives, within the framework of the existing ICT market and public-sector bodies would have required more information than was available to the working group in the time allowed. On account of the nature of the subject at hand, it was also difficult to obtain detailed data for comparison purposes from other countries.

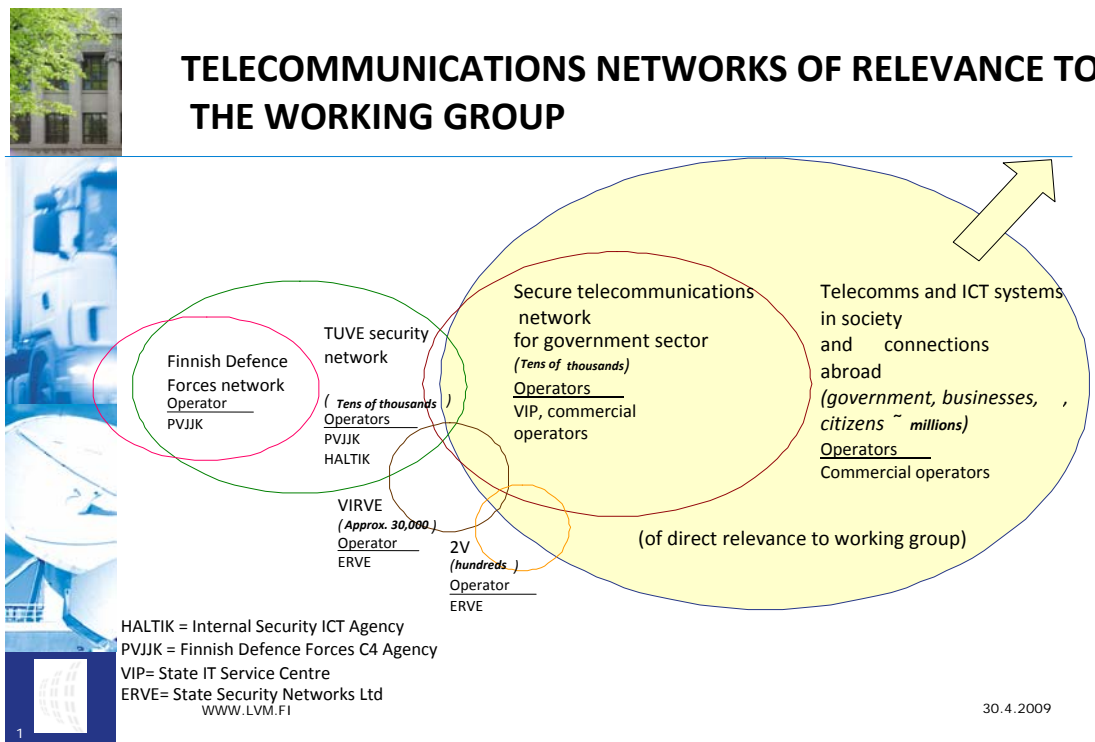


Diagram: In any society characterized as an information society, the different network and information system services available must be optimised for the purpose in question and must complement each other. The diagram illustrates in approximate terms the desired state of network and information system services.

Having concluded its work the working group hereby respectfully submits its report to the Minister of Communications.

Helsinki, 4 June 2009

Matti Lehti, chairman

Harri Pursiainen, vice chairman

Risto Volanen

Raimo Luoma

Pekka Timonen

Rauni Hagman

Ilkka Kananen

Juhapekka Ristola, secretary

Rauli Parmes, secretary

1.2 Summary

Aims of the work

The working group defined the aims of its work as follows:

ICT systems that are secure and meet the requirements concerning Finland's security of supply are an essential prerequisite for businesses, government and the everyday transactions of citizens in Finland's information society. Communications networks constitute an essential element in the networked infrastructure of society, and this has both direct and indirect effects on achievement of the fundamental aims concerning Finland's security of supply.

Basic communications services for citizens throughout the country are secured through communications policy. This policy is put into effect via legislation, operating permit regulations and other measures adopted by the authorities. The comprehensive availability of a diversity of communications networks and services can be secured most effectively by ensuring that the market functions efficiently, and especially by establishing and maintaining the right conditions for competition. Through competition, operators will have the incentive to innovate and to develop their business.

By providing technical guidance for telecommunications operators and through monitoring, the aim is to ensure that communications networks that are secure and of a high technical standard are available to users of communications services.

Current state and development needs

The working group assessed the current state and the development needs as follows:

It was necessary to take a view concerning the protection of advanced critical infrastructure under exceptional circumstances and also during serious disruptive situations in normal circumstances, on account of the following factors: society has become more information-intensive; foreign ownership has increased; functions are outsourced; ICT systems are more integrated and interdependent; usage of freely accessible information networks; and the greater dependence on electricity.

A key principle in regulating Finland's security of supply has been public-private partnership. The general security of communications networks and services is regulated by the Communications Market Act (393/2003) and the Finnish Communications Regulatory Authority's regulations issued by virtue of the Act.

Management of fixed telecommunications networks is the most critical aspect for securing functions vital to society and for the security of supply. Largely for historical reasons, the most important fixed networks by a wide margin are those of TeliaSonera Finland Plc.

The communications infrastructure consumes a substantial amount of public resources. In April 2009, the Government decided to set up a security network project for the government sector. The project is aimed at introducing a secure telecommunications network and network services for the government sector, and especially for the authorities in charge of security. The state is a significant minority shareholder in the two largest national telecommunications operators, and it also has other telecommunications holdings. Furthermore, the state is a very significant purchaser of high-quality communications services.

The development needs of services that meet the requirements for security of supply are concerned with matters such as market efficiency, regulation of product purchases, ownership and control solutions, funding for ensuring critical functions, and increasing long-term coordination. There is also a need to ensure that the state or parties under its control have sufficient ownership or control authority of a permanent nature regarding the elements of the fixed telecommunications network most critical to the functioning of society.

Proposals of the working group

With due consideration to the aims of the work and having assessed the current state and development needs, the working group decided unanimously to propose that the following measures be taken:

1. The National Emergency Supply Agency and the National Emergency Supply Organisation's information society cluster should, by the end of 2011, conduct a thorough investigation of the global and multilateral process requirements concerning contingency preparations for exceptional circumstances and for serious disruptive situations in normal circumstances, and, on the basis of this investigation, draw up a plan concerning extensive mutual cooperation between the public and private parties concerned in order to *enhance the information society's ability to withstand serious disruptions*.
2. *The legislation on contingency preparations for exceptional circumstances should be brought up to date* in line with the basic elements of the Government proposal concerning the Emergency Powers Act.
3. *National security requirements* should be included as a key component of the legislation regulating functions vital to society in normal circumstances.
4. Under the direction of the Ministry of Employment and the Economy, an investigation should be made of whether it is necessary, and even feasible in view of Finland's international obligations, to enact new legislation for ensuring that it would be possible to *monitor more effectively than at present the ownership base of companies that are important in terms of security of supply and national security in order to combat undesirable corporate takeovers*.
5. The Ministry of Transport and Communications should, by the end of 2010, draw up proposals for legislation to *reduce more effectively than at present the risks to ICT systems, and to functions vital to society that depend on these systems, posed by serious disruptive situations in normal circumstances*.
6. *Sufficient ownership and control authority of a permanent nature should be acquired for the state concerning at least those elements of the fixed telecommunications networks most critical to the functioning of society*. This objective should be implemented in such a way that, to guarantee security, the amount of the state's *capital tied up in the ownership of telecommunications operators is as little as possible*, and that the actions needed are targeted in such a way that they would not hinder the pursuit of a neutral communications policy.
7. *The Ministry of Transport and Communications should set up a standing committee of public servants*, composed of representatives of the main ministries and other authorities, for the purpose of supporting and coordinating official tasks concerning the regulation of communications markets, the availability of electronic networks for public authorities, and the ownership policy with regard to communications operators. The work of the committee should be supported by the National Emergency Supply Organisation's information society cluster. The committee would report on its actions regularly to the Ministry of Transport and Communications. The committee's reports would also be discussed in the Government's permanent secretaries' meetings and by the committee on security and defence matters.

8. In implementing the proposals set out above, the *high security national information infrastructure produced by the security network project for the government sector* should be utilised wherever possible. In addition, the requirements set out in the SOPIVA document on *contract-based contingency preparations* should be introduced throughout the government sector and in companies critical for the security of supply by the end of 2012.

2 AIMS

The working group defined the aims of its work as follows:

ICT systems that are secure and meet the requirements concerning Finland's security of supply are an essential prerequisite for businesses, government and the everyday transactions of citizens in Finland's information society. Communications networks constitute an essential element in the networked infrastructure of society, and this has both direct and indirect effects on achievement of the fundamental aims concerning Finland's security of supply.

Basic communications services for citizens throughout the country are secured through communications policy. This policy is put into effect via legislation, operating permit regulations and other measures adopted by the authorities. The comprehensive availability of a diversity of communications networks and services can be secured most effectively by ensuring that the market functions efficiently, and especially by establishing and maintaining the right conditions for competition. Through competition, operators will have the incentive to innovate and to develop their business.

By providing technical guidance for telecommunications operators and through monitoring, the aim is to ensure that communications networks that are secure and of a high technical standard are available to users of communications services.

2.1 Importance of secure communications networks

The functioning of ICT systems has become essential for ensuring the continuity of operations for all modern businesses and for the government sector. Considerable efficiency benefits have been derived and new investment opportunities emerged through the outsourcing of functions and through foreign ownership.

A characteristic feature of Finland's information society has been the very rapid changeover to mobile communications and to the use of broadband Internet connections. In the past ten years, the Internet, on-line banking, e-transactions and various electronic entertainment services have become central to the everyday lives of Finland's citizens.

It was necessary for the working group to take a view concerning the protection of advanced critical infrastructure under exceptional circumstances and also during serious disruptive situations of different kinds in normal circumstances, on account of the following factors: society has become more information-intensive; foreign ownership has increased; functions are outsourced; ICT systems are more integrated and interdependent; usage of freely accessible information networks; and the greater dependence on electricity.

Communications networks constitute an essential element in the networked infrastructure of society, and this has both direct and indirect effects on achievement of the fundamental aims concerning Finland's security of supply. These aims are to secure the functioning of society, the livelihoods of citizens and the material preconditions for national defence. Public communications networks constitute a key foundation for the communications arrangements of all of the country's public authorities, including those via dedicated communications networks.

The Government decision on safeguarding the security of supply (no. 539/2008, issued 21 August 2008) specifies the objective of securing through contingency preparations the infrastructure essential for the functioning of society and ensuring the continuity of critical production under all circumstances. Formulated on the basis of this are the objectives for protecting ICT systems during serious disruptive situations in normal circumstances and under exceptional circumstances, including a state of defence.

In April 2009, the Government decided to set up a security network project for the government sector. The project is aimed at introducing a secure telecommunications network and network services for the government sector, and especially for the authorities in charge of security, in accordance with the plan drawn up at the project planning stage.

2.2 Communications policy objectives

The underlying principle of Finland's communications policy has traditionally been to guarantee the availability of high-quality and affordable communications services and to secure basic communications services for citizens throughout the country. The means for achieving this are legislation, operating permit regulations and certain other measures pursued by the authorities, and through close cooperation between the authorities and companies in the sector. The investment-intensive nature of the sector has necessitated a long-term approach to communications policy, with the emphasis on a period of at least the next ten years.

The aim has always been that Finland's communications legislation should be technology neutral, and that the quality, price and availability of services offered to users should be optimised. The central challenge of Finland's communications policy is to create the right environment to encourage commercial suppliers to provide leading-edge services at reasonable prices while also ensuring the availability of basic communications services on the communications market regardless of where users are located in the country, even in cases where services are not commercially supplied.

The comprehensive availability of a diversity of communications networks and services can be secured most effectively by ensuring that the market functions efficiently. Competition in the sector guarantees high-quality and reasonably priced services for users, establishes sufficient incentives for operators to develop networks and services, and ensures there are opportunities for new entrants in the market.

For competition to be healthy and to function well the market mechanism must be continually in place, rewarding those companies which are able to produce goods or

services that are attractive (in terms of price, quality, availability or other aspects) to customers and consumers in their purchase decisions. Items produced on a market in which there is strong competition or the potential for such competition will meet the needs of customers and consumers in the best possible way. At the same time, society will incur the minimum of costs in striving to ensure the efficient use of economic resources.

Through competition, companies will have the incentive to innovate and to develop their business. Competition will lead to better products and further development of production, while at the same time also leading to the withering and ultimately the disappearance from the market of companies that neglect or are unable to improve the efficiency of their business. This will perpetuate the process of renewal and regeneration within the economy and maintain the transfer of resources to their most productive use, which in turn creates additional wealth in society.

By providing technical guidance for telecommunications operators and through monitoring, the aim is to ensure that communications networks that are secure and of a high technical standard are available to users of communications services.

2.3 Parties involved and operating methods

A key principle in developing Finland's security of supply has been public-private partnership. In the future, the development of ICT services meeting the requirements concerning Finland's security of supply will require ever more extensive cooperation.

There is a long tradition of partnership between the public and private sectors in Finland. The new *National Emergency Supply Organisation* operates on this very basis. The National Emergency Supply Organisation includes a planning committee network of clusters and pools. The clusters, which focus on priority areas for Finland's security of supply, are broad-based, sector-specific collaborating organisations consisting of experts representing the authorities, relevant bodies and the main parties involved. These collaborating organisations have the task of guiding, coordinating and monitoring the contingency preparations within their own particular sphere of the arrangements for the security of supply. The responsibility for the security of supply with regard to information society needs rests with the National Emergency Supply Organisation's *information society cluster*.

The *Government decision on safeguarding the security of supply* (539/2008) specifies the objective of securing through contingency preparations the infrastructure essential for the functioning of society and ensuring the continuity of critical production under all circumstances. Formulated on the basis of this are the objectives for protecting ICT systems during serious disruptive situations in normal circumstances and under exceptional circumstances, including a state of defence. The security of supply decision emphasizes the interdependence of different functions and the importance of international markets and networking for the country's security of supply. Hence, the work concerning security of supply must focus ever more strongly on national networked cooperation and on understanding the international interdependencies and the related development of contingency preparation methods.

Under the *Government resolution on the strategy for securing the functions vital to society* (23 November 2006), society must be able to secure vital functions in all circumstances. Contingency preparations emphasize the importance of making arrangements and taking measures in times of normal circumstances. In particular, electronic communications, telecommunications and energy supply systems needed for leadership and for controlling vital functions must already be protected and secured during normal circumstances, ensuring that they can withstand the demands of different disruptive situations and exceptional circumstances.

The Government resolution on the strategy for securing the functions vital to society requires that the ICT systems in use by organisations in society and by the general public are reliable and secure. The reliable operation of systems has been verified using appropriate methods and with the aid of the authorities concerned and through the cooperation of the companies involved. The data security of communications networks is in place; the basic level of security required by the legislation and regulations has been determined for communications services and basic technical systems; compliance with the regulations concerning the construction and maintenance of systems and the successful functioning of the services provided is monitored; the operating communications systems of the authorities in charge of security and those of the country's leaders are efficient and coordinated; the government's general data processing is secured; and the government sector's electronic services, data management and data security are all controlled effectively.

The Ministry of Transport and Communications is responsible for ensuring the operation of ICT systems. This means making sure that functions vital to society that are dependent on communications services, communications networks and other ICT systems are not jeopardized by disruptions in the operations of ICT systems. Through legislation, guidance, monitoring and cooperation, the aim is to ensure the construction, development and maintenance of appropriate ICT systems and to ensure as much as possible that they can be used to safeguard the data security of electronic communications and services and their usability by all service users.

The authorities are prepared if necessary to control, regulate and classify networks and their services and user groups according to their importance. Guidance is issued on the contingency preparations of telecommunications operators, and the readiness of companies is tested through supervision, inspections and contingency planning drills. The work of the Finnish Communications Regulatory Authority as the public authority with expertise and supervision responsibilities concerning protection of data in communications and data security matters is constantly being developed. Through national data security measures, cooperation between the EU's data security bodies and agencies and international cooperation, the aim is to contribute towards ensuring that there is no threat to the use of Finland's ICT systems from outside its borders. The increasing use of ICT systems is monitored to ensure that this does not jeopardise the secure control of functions in society. In ensuring the functioning of systems, developments in weapons technology are also taken into account.

Under the *Government Rules of Procedure* (262/2003), the sphere of activity of the Ministry of Transport and Communications includes electronic communications and the data security of communications services. The sphere of the Ministry of Employment and the Economy includes economic policy, the functioning of markets

and promotion of competition. The sphere of the Prime Minister's Office includes public ownership policy concerning state majority-owned and associated companies.

Under the Communications Market Act, *the Ministry of Transport and Communications determines the groups of users who are entitled to use a public authority network*. These user groups include representatives of the police, the Customs and the rescue authorities, as well as other comparable groups representing public authorities. Besides the authorities, the scope must exist for approving users who are persons not engaged in any public authority capacity but who are necessary and important for the achievement of special objectives referred to in the legislation. Such users could include individuals who are important for leadership in society, or representatives of various companies or other organisations who, in exceptional circumstances, would be charged with certain special tasks or who, even in normal circumstances, manage security tasks that are significant for the functioning of society. When approval is given for groups of users comprising persons other than those in public authorities, as referred to above, special attention should, however, be given to ensuring that these user groups do not become so large as to affect the operational prerequisites for public communications networks, thereby hindering competition on the communications market.

On 8 April 2009, the Government set up a *security network project for the government sector (known by its Finnish acronym TUVE)*. The project is aimed at introducing a secure telecommunications network and network services for the government sector, and especially for the authorities in charge of security, in accordance with the plan drawn up at the project planning stage. This project constitutes a security project. The ministries are responsible for the realisation of the project within their respective spheres of operation. A steering group is to be set up for the project and this group will later oversee the establishment of a project group. A project coordination group will also be set up later to aid the project group. The coordination group may set up cross-sectoral working groups under its direction on the recommendation of the steering group. The project began on 9 April 2009 and will be terminated on 31 December 2011. A total of EUR 197,000,000 is allocated under the main expenditure title of the Ministry of Defence in the Government's 2009 Budget for promoting network security in the government sector

2.4 Critical operating processes in Finland's information society

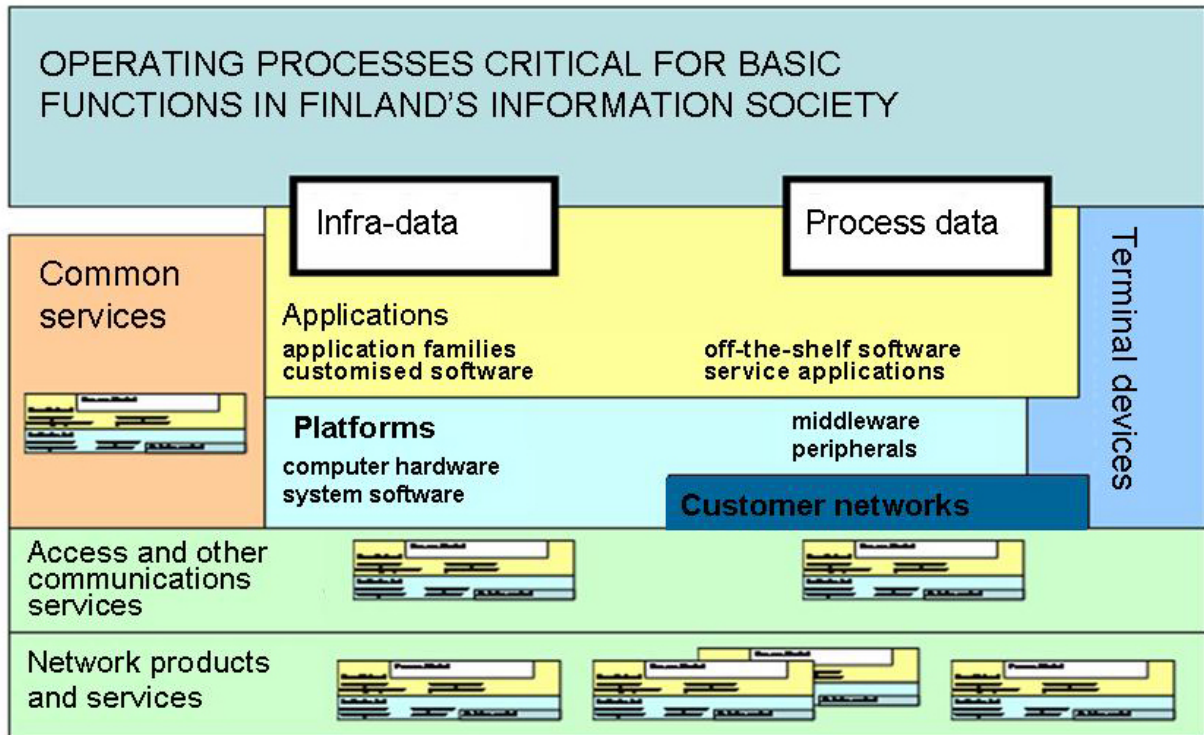


Diagram: The interconnections between information, operating processes and ICT systems are illustrated by the layers in the diagram, where a higher layer almost without exception requires the services offered by a lower level. Process data refers to information processed by the end user in the operating process. Infra-data refers to information that is copied and distributed for the purpose of combining or handling it with process information.

In Finland's information society, ICT plays two different roles in the activities of telecommunications operators and organisations: an implementing role and an enabling role. ICT can be used to support and improve the efficiency of existing structures and processes. ICT can also enable new types of operating model and, in extreme cases, it could even change the structure of an entire industry.

The operation of all intelligent systems is based on different levels of information. Systems need information on the world around them; they interpret this data within their own framework; and, through their actions or by distributing information, they have an impact on other systems. The structure of a system, in terms of the information it holds and processes, consists of its physical components, their relationship to each other, and the data stored in the system. The extent of computerised equipment and systems in Finland's information society highlights the essential nature of information.

The computer-based processes rely on various software applications, which at their simplest are off-the-shelf packages requiring no user-specific customisation. At the other extreme are extensive families of software applications, which can be complex and purpose-specific software packages.

Any information society will be reliant on information processes. Typically, the entire process must function successfully in order that a certain desired action or service is properly available. However, the more critical a specific function in the process, the greater will be its impact. In terms of the functioning of the information society, network products and services constitute a critical element of this.

3 CURRENT STATE AND DEVELOPMENT NEEDS

The working group assessed the current state and the development needs as follows:

It was necessary to take a view concerning the protection of advanced critical infrastructure under exceptional circumstances and also during serious disruptive situations in normal circumstances, on account of the following factors: society has become more information-intensive; foreign ownership has increased; functions are outsourced; ICT systems are more integrated and interdependent; usage of freely accessible information networks; and the greater dependence on electricity.

A key principle in regulating Finland's security of supply has been public-private partnership. The general security of communications networks and services is regulated by the Communications Market Act (393/2003) and the Finnish Communications Regulatory Authority's regulations issued by virtue of the Act.

Management of fixed telecommunications networks is the most critical aspect for securing functions vital to society and for the security of supply. Largely for historical reasons, the most important fixed networks by a wide margin are those of TeliaSonera Finland Plc.

The communications infrastructure consumes a substantial amount of public resources. In April 2009, the Government decided to set up a security network project for the government sector. The project is aimed at introducing a secure telecommunications network and network services for the government sector, and especially for the authorities in charge of security. The state is a significant minority shareholder in the two largest national telecommunications operators, and it also has other telecommunications holdings. Furthermore, the state is a very significant purchaser of high-quality communications services.

The development needs of services that meet the requirements for security of supply are concerned with matters such as market efficiency, regulation of product purchases, ownership and control solutions, funding for ensuring critical functions, and increasing long-term coordination. There is also a need to ensure that the state or parties under its control have sufficient ownership or control authority of a permanent nature regarding the elements of the fixed telecommunications network most critical to the functioning of society.

3.1 Current state

3.1.1 Availability of communications networks and services

The availability of communications networks can be divided on the basis of three different network categories: core networks, regional networks and access networks. The *access network* is the network to which end users connect; internal networks in buildings are also considered part of the access network. An often-used synonym is access technology. The following are examples of access networks or access technologies: fixed copper connections, cable television networks, optical fibres,

WLAN, GSM, UMTS, wireless broadband @450 and xDSL. The service coverage of individual access networks is usually relatively small.

Access networks are connected to each other typically by combining a group of access networks into a *regional network*, also widely known as a *metro network*. Major customers can also connect directly to a metro network, and in doing so may be offered higher speed communications. Regional and access networks are used somewhat interchangeably. The term *local network* is used to refer normally to the fixed copper networks of regional telecommunications operators, through whose subscriber connections various communications services, such as broadband subscriptions, can be offered to users.

The core network is a data transmission network connecting towns and cities and other municipalities, and different regional or access networks. At the core network level, services are based on the fixed optical core network, which covers all the most important population centres. The optical fibre core network includes backbone routers, the transmission links between them, and peripheral routers that use various technologies to connect the access networks to the core network. The task of the core network is to transfer data between access networks as rapidly and reliably as possible.

Network model - Logical structure

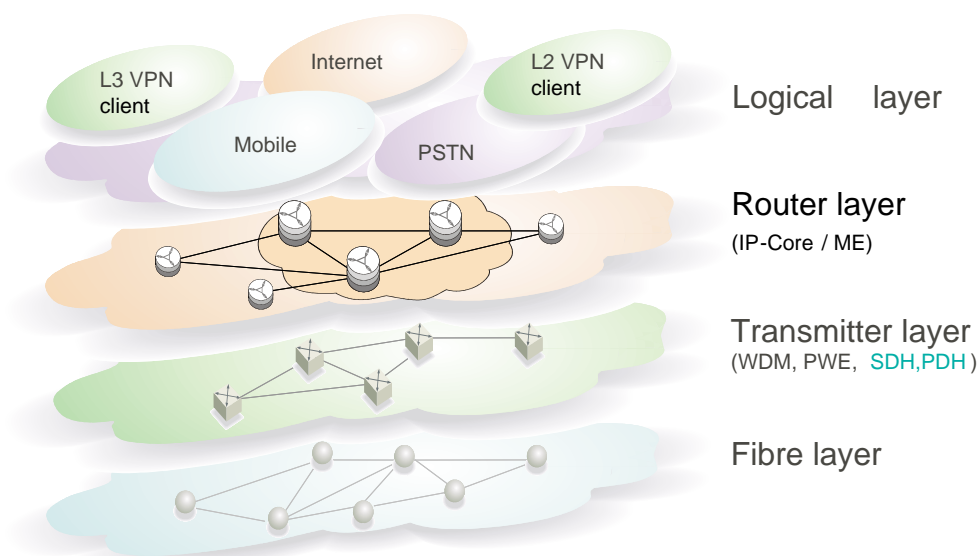


Diagram: The diagram shows the logical structure of communications networks. The higher the layer in the structure, the closer it is to the individual user. The lower the layer, the greater the number of users concerned. Lower level services are needed in order that the upper level services which rely on them can function. The fixed telecommunications network nodes that are the most critical to society are located in the lower part of the diagram.

There are five core networks in Finland, namely those of TeliaSonera, Elisa, DNA, TDC Oy and Finnet Group. Network coverage overlaps in the major urban areas, whereas in northeast and northern Finland there is only one core network, that of TeliaSonera.

The core network nodes are found in the largest urban areas. These provide access points for local network connections or offer the opportunity to access national

services such as mobile and fixed network phone services and Internet and data connections. Those in control of core network connections can offer their customers corporate services with virtually nationwide coverage. Indeed it is via core networks that telecommunications operators can provide broadband services outside their own traditional geographical areas by leasing some of the network capacity of another party by means of DSLAM technology.

In the biggest cities the telecommunications operators have begun to offer their own fast 100 Mbit/s optical fibre connections in their competitors' territories, even obviating the need to lease copper connections from a local telecommunications operator.

Besides competition between networks, the competition between technologies on the communications market is increasing, because broadband services, for instance, can be produced using DSL, cable, fibre or wireless technology, and phone services are produced via the traditional fixed network, a mobile network or with VoIP technology. Text-based communications can be transmitted by e-mail, SMS or instant messaging.

Overall, the conclusion is that today's competition-based communications market in Finland has been of great benefit to end users, especially in the broadband and mobile markets. By European standards, the uptake of services has been at a record pace, and prices are low in relation to those of countries featuring in comparisons.

Developments in technology have also kept pace well by European standards: 3G services have been taken up quickly, and optical fibre networks are already available to users in the major urban areas. In mobile communications, services are provided on a competitive basis throughout the country, and competition exists in broadband services in all the bigger urban areas. At the end of 2010, wireless broadband with a speed of at least 1 Mbit/s will be available to 99.9% of the Finnish population.

In services for corporate and institutional customers, competition has been even more successful than in consumer services. The telecommunications operators managing the core networks are able to offer a full range of communications services, at least to their biggest customers: fixed and mobile network phone services and various data services. In addition to communications services, telecommunications operators are often able to offer corporate and institutional customers other ICT services too, and also systems integration, because in practice communications services need to be integrated with the customer's information systems, such as production and sales control systems.

Functions requiring security of supply use not only public communications networks and the VIRVE public authority network, but also their own separate local, regional and national radio networks. These networks are found especially in the production, transmission and distribution of energy, in water supply, municipal engineering, transport logistics, production for the export industry, and in food supply. In terms of the legislation concerning the communications market, these are seen mainly as networks offered to a pre-restricted group of users, thus not constituting public telecommunications and not falling within the scope of the Communications Market Act, except in regard to the regulation of disruptions.

Management of fixed telecommunications networks is the most critical aspect for securing functions vital to society and for the security of supply. The most important fixed networks by a wide margin are those of TeliaSonera Finland Plc. The Elisa Oyj network is also of considerable significance. Of lesser significance, though still important, are the fixed networks of DNA Ltd and certain other telecommunications operators (Finnet, TDC). TeliaSonera Finland Plc is clearly the most important provider of broadband services in sparsely populated areas, and the effective implementation of the Government's broadband policy is in no small way dependent on the actions of the company.

Both *Appendix 2*, concerning security networks, threat scenarios, contingency preparations and network structure in detail, and *Appendix 3*, concerning critical states and connections in detail, remain confidential on the basis of paragraphs 7, 8 and 20 of section 24 of the Act on the Openness of Government Activities.

3.1.2 Changes occurring in communications networks and markets

Certain general tendencies are evident in the *business decisions of telecommunications operators* which could also affect the security of supply in regard to network and communications services. Various ownership and cooperation arrangements between telecommunications operators are continuing, and in electronic communications networks this could lead to larger companies operating nationwide in Finland or across several countries. This process will also give rise to more specialised operators. In addition, the ownership base of telecommunications operators is becoming more fragmented and more international. The establishment of greater international links can also be seen in the decisions to locate abroad the active components of communications networks and services. The growing demand for returns is also evident in the opportunities for investing in enhancing the security of communications networks and services to a standard above the minimum requirements set by law.

Of special interest for the security of supply is the increase in subcontracting, for instance in network servicing, maintenance and repair work. The concentration of these activities has also led to the outsourcing of functions throughout the sector to just a handful of operators, which could be problematic for service availability in the event of a large-scale crisis. In subcontracting agreements, the clauses concerning security, responsibilities and information flow are not always sufficiently clear and comprehensive by any means.

As a consequence of the growth in subcontracting, the specialisation of telecommunications operators and the emergence of separate network and service operators, the division of responsibilities in the service chain is becoming more fragmented. This, in turn, is adding to the need for greater expertise in procurement. In communications networks and services, reference is often made to end-to-end functionality, which refers to the interoperability of the networks and services of different operators. The same approach on a larger scale is also helpful in envisaging needs in regard to security of supply.

Clear trends in the *development of technology* include network integration, the spread of IP-based technology, and the wider use of wireless access networks and other new wireless applications.

Communications services and access networks focus on the same core networks. Concentration is also occurring in hardware solutions and network management. Different networks can have common, centralised components and common hardware facilities. As communications networks become more integrated, services are becoming more vulnerable, because an individual fault can have a large scale impact on the operation and usability of communications networks and services.

Solutions based on the Internet and on next generation networking (NGN) are being utilised in the production, distribution and management of communications services. These Internet and NGN models compete with each other to a certain extent. The Internet model is based on software installed in a terminal device, enabling global service provision to customers who are linked to the Internet. The operator-focused NGN model is based on the telecommunications operators having intelligent and functional networks and network equipment, guaranteeing service quality but at a significantly higher cost.

Services are increasingly Internet-based, i.e. software-based. At the same time, IP-based technology is gaining ground in communications services and in core networks: voice services, for example, are becoming IP-based, and core networks are using IP-based MPLS technology for carrying traffic. IP-based services are susceptible to human error in specification setting, which can have major implications in an integrated network.

Service vulnerability due to the increase in network integration and IP-based technology, together with the fragmentation occurring among providers, is making the management of faults and disruptions in communications networks more difficult. When a fault occurs, both the customer and the telecommunications operator can find it difficult to establish quickly the cause of the problem. In the operation of critical infrastructure, the usability of services and the continuity of operations must be ensured under all circumstances. To guard against faults and disruptions, the agreements made must take into account not only the various backup and contingency preparation arrangements but also the need for information flow to be as quick as possible and the need to be able to contact the right people quickly.

The increase in IP technology and wireless networks and the fragmentation among providers will also add to the data security risks. Since functions that are critical for the security of supply are heavily reliant on public communications networks and services, their data security requirements are very considerable. This is primarily because the service chain can consist of a number of different operators, and the systems of operators that are critical for the security of supply can be exposed to threats emerging via the public network. Furthermore, providers of a minor service forming part of a large service entity are not necessarily able to meet data security requirements in full.

In the local networks of companies and other organisations, cable networks that are expensive to install and maintain are being replaced with less costly wireless sensor

networks. Another new technology, radio frequency identification (RFID), is allowing many new logistics applications in industry, commerce and transportation. The use of these technologies will become more widespread over the next few years.

Along with the changes in technology, climate change could also have an impact on the security of communications networks and services if there is an increase in weather phenomena that cause disruptions, such as storms and floods. Tolerance of normal climate-related disruptions is already part of the basic requirements for the technical standard of communications networks and services, but any increase in disruptions will have an impact, especially on the provision of services that meet the requirements concerning Finland's security of supply.

There are many critical components in communications networks and services. These can include telecommunications terminal devices, network products and services, and access and other communications services. The physical location of equipment and systems is also of major significance for security. The facilities in which equipment is housed and the appropriate protection of those facilities are of particularly acute importance when they are used by a number of different parties.

The security-critical components and factors referred to above are all concentrated in the same core networks. For everything to function reliably, it is essential that the main fixed telecommunications networks continue to operate under all circumstances. For this reason it is the security of fixed telecommunications networks that represents the most critical aspect in Finland's information society.

There is no sign of any developments in *consumer behaviour* or in the provision of communications services that would have a particular impact on Finland's security of supply. The most significant change occurring internally is that traditional communications services are being offered via the Internet at lower prices than before, and even at no charge. Competition in services is becoming separate from network competition, and service provision is becoming more global. Many consumers are now using Finnish or foreign IP-based services (Gmail, Skype, Messenger) that are low cost or free of charge. There is also an increase in community-based on-line activity, not only in the sharing of content but also of infrastructure. Some of these services are beyond the reach of Finnish communications market regulation, either because the technical provision is independent of any telecommunications operator or because the provider is located, and the service provided, abroad.

In traditional communications services it is noteworthy that, in addition to the long-observed high level of penetration in mobile subscriptions, there has been considerable growth in broadband subscriptions, transfer to wireless services, and a continuous reduction in fixed phone network subscriptions.

The need to ensure the availability and usability of the frequency resources of most importance for the security of supply is also an area that requires *international cooperation*. The availability of the new broadband radio networks requires harmonised frequency solutions that are regional or global. At both the global and the European level there are also projects emerging around the world that could, when in operation, have an adverse effect on the usability of frequencies in Finland. It is thus essential to contribute to the preparations for international decision-making on

frequencies, to follow the work on this via the ITU and CEPT working groups, and to respond to projects at a sufficiently early stage.

It is also essential to ensure that the radio network frequencies of parties safeguarding Finland's security of supply are protected from disruption. The need for protection is particularly acute in regard to using the radio system frequencies of public authorities and of certain businesses, and those used in aviation, shipping, meteorology and energy supply. Public authorities recognise a need to improve the efficiency of their actions in combating threats of different kinds, and this emphasizes the importance of secure communications systems.

3.1.3 Legislation

The general security of communications networks and services is regulated by the *Communications Market Act* (393/2003) and in the Finnish Communications Regulatory Authority's regulations issued by virtue of the Act. The Communications Market Act (section 128) sets out the fundamental duty to plan, build and maintain communications networks and services in such a manner that they can withstand normal climatic, mechanical and electromagnetic interference and function as reliably as possible even in disruptive situations under normal circumstances and in exceptional circumstances.

In section 129 of the Act, the Finnish Communications Regulatory Authority is authorised to regulate in more detail the various technical quality and interoperability considerations in communications networks and services, as given in the 21-item list set out in the section. Regulation number 54 of the Authority, on the protection of communications networks and services, is key in ensuring security. It obligates telecommunications operators to attach a priority rating to their systems and system components and to ensure that they have properly functioning equipment, power supply and physical security arrangements, and to organise reserve routes in accordance with the rating. The priority rating is based on the number of users affected by any malfunctioning element or on the size of geographical area concerning the user services affected, or on the type of services affected. The special needs of individual users therefore have no effect on the priority rating or the contingency preparation obligations. Within this regulatory framework, products meeting the requirements concerning security of supply must emerge on market terms. Chapter 9 of the Communications Market Act sets out provisions concerning telecommunications operators' contingency preparations for exceptional circumstances.

Parties offering *information system services* are not subject to such contingency preparation obligations. Legislative opportunities for reducing the effects of serious disruptions under normal circumstances are currently very limited.

3.1.4 International comparison

The supply of and demand for communications networks that are secure and meet the requirements for Finland's security of supply are strongly linked to the need to ensure national security and the country's capacity to function. Hence, most information on the subject is naturally confidential and is available to only a limited circle even

within the country. Obtaining detailed international comparison data is practically impossible. However, through public information sources and direct contacts it is possible to obtain general information and to identify certain basic principles in the different national approaches.

In the European Union, the issue has been dealt with in various different contexts, the latest being a Commission communication concerning critical information infrastructure protection (COM 2009/149). This stresses prevention, contingency planning and awareness, and specifies a series of direct measures for improving the security and resilience of critical information infrastructure. The communication's purpose is to help develop European policy to bolster security and reliability in an information society framework. The communication states that enhancing the security and resilience of critical information infrastructure will require the resolution of a number of challenges, among them the incoherent and uncoordinated nature of the different national approaches, the need for a new European management model for critical information infrastructure, Europe's limited advance warning and response readiness, and international cooperation.

One existing element in regional cooperation at international level is the Meridian process (<http://www.meridian2007.org>), in which Finland is one of the countries involved. This is a restricted forum for national governments, set up for the exchange of confidential information on matters related to securing critical information infrastructure.

In planning the measures for enhancing the security of supply of communications networks, it is important to take factors such as the following into account: a) the key functions that should be protected; b) threats concerning the key functions; and c) the structure of communications networks and markets as part of the critical infrastructure. As these factors can vary from one country to the next, the usefulness of detailed international comparison data is questionable, even if this were available.

Many countries have drawn up strategies for securing critical infrastructure and critical information infrastructure. These strategies identify the critical nature of the infrastructure in terms of the functions vital to society, and the threats concerning infrastructure. Scattered information gathered from public information sources indicates that definition of the interdependencies between critical functions and critical infrastructures in society has been a common challenge. Many countries have found that at a general level there is a strong interdependence between energy supply and communications networks, for instance, but a closer analysis of this is not available from public information sources.

Financing, administrative and legislative models differ between countries. Although detailed information on different countries is not available, the models can be divided as follows in terms of their main principles: 1) obligations for securing functions have been established for those parties that are critical for the functioning of society. The costs are the responsibility of the parties themselves; 2) obligations for securing functions have been established for those parties that are critical for the functioning of society. The costs are reimbursed in full or in part; 3) obligations for securing functions have been established for telecommunications operators offering telecommunications connections to parties that are critical for the functioning of

society. The costs are met in full by the telecommunications operator; 4) obligations for securing functions have been established for telecommunications operators offering telecommunications connections to parties that are critical for the functioning of society. The costs are reimbursed in full or in part.

On the basis of information obtained from *Sweden's* Post and Telecom Agency, the following can be concluded about developments in the security of supply of Sweden's communications networks. Previously resources were devoted to the functioning of communications networks in order to secure the resource needs of the country's defence forces in a crisis situation. The Agency has drawn up a new strategy on the robustness of communications networks and the prevention of weaknesses in the networks. The aim of the strategy is to maintain and improve the functioning and robustness of communications services. Peacetime crises must not be allowed to lead to major interruptions and disruptions in communications networks. Major adverse effects should be avoided in crisis situations, and there should be an opportunity to take into account changes in the security situation every 5-10 years. The objectives are to be achieved through cooperation between the government and operators.

The tools for coordination in Sweden are information exchange, joint crisis drills and shared systems. Resources are also devoted to training, and the country is an active participant in standardisation efforts and international cooperation. To enhance the robustness of the network, a proposal has been made for increasing the number of nodes in the fixed network. Additional network connection points are also considered necessary, so that different operator networks could be connected, if required, and traffic volumes balanced out. The strategy states that exchanges and other network equipment should be located in better protected premises with a power supply that is secure in crisis situations.

Under the legal provisions of a decree, network operators with a turnover exceeding SEK 30 million and with networks that are significant have to pay the Agency a contingency planning charge. Through this charge a sum of approximately SEK 100 million is collected annually. The charge is a maximum of 0.04% of the company's turnover. In addition, the state can, if necessary, grant budget funding channelled via the Agency. The Agency purchases the necessary services from the private sector.

3.1.5 Government investment in the ICT sector

The ICT infrastructure consumes a substantial amount of public resources. Examples include:

- 1) the state owns 13.72% of TeliaSonera AB (via Solidium), which, on 31 March 2009, was equivalent to EUR 2,224.1 million;
- 2) in the third supplementary budget of 2008, a total of EUR 196 million was allocated for the purchase of Elisa Plc shares; the state owns 9.62% of Elisa Plc, which, on 10 May 2009, was equivalent to EUR 166.5 million;
- 3) in a meeting of the Cabinet Committee on Economic Policy in December 2008, the Government decided that the amount of broadband subsidy for telecommunications operators should be a total of EUR 66 million for the period 2010-2015;

- 4) under the 2009 budget submission a sum of EUR 197 million is to be used for the construction of a state security network;
- 5) the state owns 60% (2007) of Corenet Ltd (via VR Ltd). The company's turnover was EUR 31.4 million;
- 6) the state owns 100% of State Security Networks Ltd. The company's turnover was EUR 26 million; and
- 7) the government authorities in charge of security, and other public authorities, have their own extensive communications networks and information systems.

Furthermore, the state is a very significant purchaser of high-quality communications services.

3.2 Development needs

3.2.1 Identifying parties that are critical for the security of supply

The parties critical for security of supply are all different in terms of their importance, size and resources. In securing network and communications services that meet the requirements concerning Finland's security of supply, the first step is to identify the parties that are critical for security of supply and which elements of their activities are critical. It is then possible to identify which element of the operations is dependent on the communications network or service. A party that is critical for security of supply does not necessarily see itself in this role. Furthermore, the existence of a chain of subcontractors may mean that the critical nature of some part of the chain is not necessarily recognised.

Taking into consideration the security of a service when procuring communications services and networks requires a degree of expertise. A party that is critical for the security of supply needs information about both its own needs and the services available if it is to be able to use security and quality as procurement and tendering criteria. Parties also need to be able to assess overall whether they can rely on one solution or the solutions of a single service provider, or whether they should acquire several, mutually verifying services. A service that meets the requirements for the security of supply is a package consisting of, for instance, special electrical and physical security of network components, organisational security of the service provider, knowledge of the entire service chain, and the customer service level (e.g. ease of contacting appropriate persons)

3.2.2 Cooperation

The development of network and communications services that meet the requirements concerning Finland's security of supply requires the cooperation of all concerned. In the public and private sectors the needs of the parties involved must be analysed, their awareness of the communications infrastructure must be enhanced, and demand must be focused on communications network and service features that best serve security of supply. This may best succeed through well-coordinated cooperation between

telecommunications operators, the parties critical for security of supply, and the authorities. The cooperation among public authorities is especially reliant on the extent of any public funding concerning facilities, structures and features of communications networks and services, because the competition angle and government sector cost pressures must be taken into consideration in this.

The introduction of technical or service configurations designed to enhance the security of supply can in some cases be more effectively promoted on a centralised basis rather than merely through agreements of individual parties. Procurement could, for instance, be centralised, focusing on a number of parties that are critical for security of supply. Procurement could be simply coordinated in the form of joint purchasing or it could also be financed from public funds.

In general terms, the tools for developing services that meet the requirements concerning Finland's security of supply include more effective marketing, regulation of products available, ownership solutions and financing.

3.2.3 Utilising market mechanisms

In developing the supply of services that meet the requirements concerning Finland's security of supply, as much use as possible must be made of marketing mechanisms in order that services are produced cost-efficiently.

Services that are tailored and verified on the basis of commercial principles could take into consideration requirements for security of supply that exceed the basic level associated with services available on the market. The first precondition for improving the efficiency of transactions is to enhance the awareness of parties critical for the security of supply about their own roles and about which of their functions are critical to society at large. The demand for and supply of secure services can be boosted if purchasers have at their disposal pre-prepared information on the service's security features, and if telecommunications operators have at their disposal pre-prepared model contracts.

In the SOPIVA project, launched in 2005 jointly by the National Emergency Supply Organisation's information network, IT and electronics pools, a study was made of contract-based contingency preparations in the information society cluster. The focus was on establishing contracts for business profitability assessments, and emphasis was given to the fact that security means improving the basic level of network security.

3.2.4 Legislation

The main administrative branches of government should formulate legislative projects for political consideration that could be used to create the conditions for minimising more effectively than at present the effects of serious disruptions under normal circumstances on functions vital to society. Bringing the legal provisions up to date in line with the general legislation on security of supply and the competition legislation would be a way of improving the security of supply of communications networks and services in situations in which the market cannot produce adequate services.

Via the mechanisms of the legislation on security of supply it should be possible to identify and name the parties and functions that are critical for the security of supply. The legislation on the communications market would be the most natural place for the necessary instruments for establishing rights and obligations in regard to communications networks. The alternatives to establishing obligations would be company-specific resolutions and general obligations set out in legal provisions, for instance on contingency preparations for certain service provision. In addition, there may be a need for the legislation on security of supply and on the communications market to set out grounds consistent with the competition legislation for cost reimbursement and the exercise of authority. A very significant factor in developing the security of supply of networks and services in practice is the allocation of responsibility for the costs of security of supply.

The legislation on contingency preparations for exceptional circumstances should be brought up to date in line with the basic elements of the Government proposal (3/2008) concerning the Emergency Powers Act. The Government proposal states that under exceptional circumstances it is essential to secure the supply of communications services because the importance of communications is merely heightened in a crisis situation. Most of the functions vital to society are today dependent on the functioning of ICT systems. The functions vital to society include power and water distribution, financial services, energy production facilities, data transmission and other services in a key position during a crisis without which citizens and businesses could not function.

Under the provisions set out in the Government proposal, the Ministry of Transport and Communications could, with the purpose of ensuring well-functioning ICT systems and securing functions vital to society under exceptional circumstances, decide to obligate a telecommunications operator to produce network and communications services and to provide public authorities with a status report on the use of these services, to obligate a telecommunications operator to produce communications services in a certain geographical area or to produce certain services such as maintenance of mobile networks; or, if exceptional circumstances prevail, obligate a telecommunications operator to keep communications networks in good condition or build or refrain from building communications networks, or connect one communications network to another or to dismantle a connection; or obligate a telecommunications operator to cut network connections or communications service connections to a certain country or to international network and communications services for a defined period or until further notice.

The requirements of national security should be incorporated as a key element of legislation for normal circumstances where the effects of this legislation are felt in functions vital to society.

The Government proposal for legislation on auctions for certain radio frequencies (37/2009) includes a proposed procedure by which operating permits would always be granted to the highest bidder. However, at the same time it is proposed that there be a provision to the effect that an operating permit would not be granted or its transfer approved if there is justified cause to suspect that the granting or transfer would have an adverse effect on national security. For the purpose of assessing the effects on national security, the Government could request opinions on the matter from, for

instance, the Finnish Defence Forces or the Finnish Security Police, to supplement its own assessment. Corresponding provisions should also be incorporated in other key items of legislation for normal circumstances.

3.2.5 State ownership in the communications market

The state's ownership interests are nowadays concerned both with finances and ownership consolidation goals. The state does not, however, have any control or influence over the functions that are genuinely the focus of its ownership interest. Put another way, the state owns shares in the parent companies of telecommunications operators that own networks but has no direct control over these operators' communications networks.

Nevertheless, the state's highest level of leadership and other authorities in charge of security under the crisis management arrangements, such as the Finnish Defence Forces and authorities responsible for public order and security (e.g. the police and the Finnish Border Guard and the rescue authorities), must have at their disposal a security network with a high protection rating. There is also a need to ensure that the state or bodies under its control always have sufficient ownership or control authority regarding the elements of the fixed telecommunications network most critical to the functioning of society.

The state's ownership interests can of course change over time. The debate currently in progress emphasizes communications networks rather than service operators. Though this is closely in line with ownership policy and its main focus areas, it does not fully correspond to the prevailing situation. In the future, it would be more natural for the state to be involved in the ownership of infrastructure than the ownership of commercial parties that utilise the infrastructure. Correspondingly, most of the state's non-financial ownership interests in telecommunications operators engaged in service activities would be removed if the main network infrastructure were separated from those engaged in service activities, or if other solutions were introduced that would secure the continuity of vigorous service competition.

4 PROPOSED DEVELOPMENT MEASURES AND THEIR EFFECTS IN BRIEF

With due consideration to the aims of the work and having assessed the current state and development needs, the working group decided unanimously to propose that the following measures be taken:

1. The National Emergency Supply Agency and the National Emergency Supply Organisation's information society cluster should, by the end of 2011, conduct a thorough investigation of the global and multilateral process requirements concerning contingency preparations for exceptional circumstances and for serious disruptive situations in normal circumstances, and, on the basis of this investigation, draw up a plan concerning extensive mutual cooperation between the public and private parties concerned *in order to enhance the information society's ability to withstand serious disruptions.*

Such an investigation would support the legislative projects by producing empirical information, particularly on network interdependencies the identification of which is essential for ensuring security. Function-specific pilot investigations would also support the process of planning the necessary cooperation.

Cooperation is one of the important factors in terms of managing the functions vital to society in situations where society is threatened by a serious event. Even where a serious disruption is already occurring, cooperation to restore a level of equilibrium to the management of the situation is essential, too. Preliminary planning would guarantee that the cooperating parties are able to react and function in accordance with known operating models. This is a matter of both anticipatory planning for continuity and furtherance of the recovery process.

The investigation would also provide a description of how the functional capacity of the authorities can be strengthened in managing disruptive situations in communications networks and services and in assembling a status report and providing information about it. An appropriate status report would also be of key importance for minimising the adverse effects of disruptive situations and for accelerating the recovery from such situations. Progress reports on the investigation must be submitted to the standing committee of public servants referred to below.

Drawing up a plan that can be implemented requires extensive expertise on the part of those concerned as well as their commitment to the project, and also an openness to finding new ways of resolving issues. The collaborative planning undertaken by the National Emergency Supply Organisation could be utilised in the work of the standing committee of public servants proposed below.

No extraordinary financial or legislative impacts are anticipated with this proposed measure.

2. The legislation on contingency preparations for exceptional circumstances should be brought up to date in line with the basic elements of the Government proposal concerning the Emergency Powers Act.

The Government proposal concerning a new Emergency Powers Act (3/2008) was presented to Parliament in February 2008. The proposal includes additional and respecified powers for the authorities, in part to bring these powers into line with the threat scenarios posed, as required by the strategy for securing functions vital to society.

The renewal of the Emergency Powers Act is of primary importance. The existing Emergency Powers Act contains no separate provisions on ICT systems. It is expected that the revision of the regulations in the Emergency Powers Act will clarify and ease the efforts of the authorities to plan and make contingency preparations for exceptional circumstances.

Under the provisions set out in the Government proposal, the Ministry of Transport and Communications could, with the purpose of ensuring well-functioning ICT systems and securing functions vital to society under exceptional circumstances, decide to obligate a telecommunications operator to produce network and communications services and to provide public authorities with a status report on the use of these services; obligate a telecommunications operator to produce communications services in a certain geographical area or to produce certain services such as maintenance of mobile networks; or, if exceptional circumstances prevail, obligate a telecommunications operator to keep communications networks in good condition or build or refrain from building communications networks, or connect one communications network to another or to dismantle a connection; or obligate a telecommunications operator to cut network connections or communications service connections to a certain country or to international network and communications services for a defined period or until further notice.

The Emergency Powers Act will not give rise to any significant costs in normal circumstances, though the costs that would be incurred would be in contingency preparations for exceptional circumstances, such as contingency planning drills and drawing up contingency plans. The proposed Emergency Powers Act would not alter the scope of the contingency preparation obligation, and so the costs of such preparations are not expected to change from the present situation. In addition, the contingency preparation obligation under the Emergency Powers Act would in future continue to apply only to public sector bodies.

Under exceptional circumstances, in which the powers conferred by the Emergency Powers Act would apply, the Act could have quite significant financial implications, depending on the type of exceptional

circumstances in question. An accurate assessment of these costs is not possible, however.

Discussion of the Government proposal for a new Emergency Powers Act will continue in Parliament during the next parliamentary session.

3. *National security requirements* should be included as a key component of the legislation regulating functions vital to society in normal circumstances.

Finland's security of supply will improve with legislation which ensures that communications networks and services meet national security requirements. This would mean that communications networks and services are reliable and that they function reliably both in disruptive situations in normal circumstances as well as under the exceptional circumstances referred to in the Emergency Powers Act.

This aim is already incorporated in the Government proposal for legislation on auctions for certain radio frequencies (37/2009), which includes a proposed procedure by which operating permits would always be granted to the highest bidder. However, it is also proposed that there be a provision to the effect that an operating permit would not be granted or its transfer approved if there is justified cause to suspect that the granting or transfer would have an adverse effect on national security. For the purpose of assessing the effects on national security, the Government could request opinions on the matter from, for instance, the Finnish Defence Forces or the Finnish Security Police.

4. Under the direction of the Ministry of Employment and the Economy, an investigation should be made of whether it is necessary, and even feasible in view of Finland's international obligations, to enact new legislation for ensuring that it would be possible to *monitor more effectively than at present the ownership base of companies that are important in terms of security of supply and national security in order to combat undesirable corporate takeovers.*

In some EU member states and in Russia, for instance, there are restrictions on foreigners owning companies that are strategic in terms of the functioning of society. In the case of Russia, a foreigner is only permitted to own less than half of the share capital of a telecommunications operator.

In Finland, an examination of the need for and feasibility of similar arrangements should be conducted.

5. The Ministry of Transport and Communications should, by the end of 2010, draw up proposals for legislation to *reduce more effectively than at present the risks to ICT systems, and to functions vital to society that depend on these systems, posed by serious disruptive situations in normal circumstances.*

In situations where problems are specifically concerned with the functioning of ICT systems, the powers under the proposed new

Emergency Powers Act would only be available under exceptional circumstances, where the situation regarding security in society is already extremely serious.

The powers concerning normal circumstances as they are understood today could prove insufficient in serious disruptive situations. This could in turn greatly jeopardise the operation of functions vital to society.

Contingency preparations must be made in advance, in normal circumstances, and they must therefore be based on legislation applying to normal circumstances, the continued development of which is essential. A project should be launched in which new provisions applicable to normal circumstances ensure the establishment of clearly defined powers in order that the necessary measures for managing a threat caused by serious disruptive situations, or for managing the situation itself if this is already at hand, can be launched as quickly and efficiently as possible. This would further the aims for security of supply such that functions vital to society could, not only under exceptional circumstances but also in serious disruptive situations, be maintained as close to their normal state as possible, and that the effects of a serious disruptive situation could be reduced and management of those effects improved.

There could be a considerable need for change concerning statutes pertaining to the legislation on communications policy, because the current regulations concern contingency preparations for normal and exceptional circumstances. Currently the regulations do not cover the 'grey area' in which the exceptional circumstances referred to in the Emergency Powers Act are not yet relevant but where the situation is so serious that government actions are absolutely critical.

The proposed measure could have financial implications in areas covered by the obligations of the new legislation.

6. Sufficient ownership and control authority of a permanent nature should be acquired for the state concerning at least those elements of the fixed telecommunications networks most critical to the functioning of society. This objective should be implemented in such a way that, to guarantee security, the amount of the state's capital tied up in the ownership of telecommunications operators is as little as possible, and that the actions needed are targeted in such a way that they would not hinder the pursuit of a neutral communications policy.

The working group assessed three quite different approaches to ownership policy.

For each approach the following were specified: the main actions, the effects on security of supply, the financial effects, the need for legislative changes, and the effects on economic growth and innovation.

Common to the alternatives is that each could be used to promote the availability of communications networks that are secure and meet the requirements concerning Finland's security of supply. The alternatives differ from one another considerably, especially in regard to the amount of capital investment from the state and the impact of competition.

The working group concluded by proposing that a single alternative be consistently pursued. Appendix 1 is confidential on the basis of paragraphs 7, 8 and 20 of section 24 of the Act on the Openness of Government Activities.

7. The Ministry of Transport and Communications should set up a standing committee of public servants, composed of representatives of the main ministries and other authorities, for the purpose of supporting and coordinating official tasks concerning the regulation of communications markets, the availability of electronic networks for public authorities, and the ownership policy with regard to communications operators. The work of the committee should be supported by the National Emergency Supply Organisation's information society cluster. The committee would report on its actions regularly to the Ministry of Transport and Communications. The committee's reports would also be discussed in the Government's permanent secretaries' meetings and by the committee on security and defence matters.

Cooperation among the various parties would ensure sufficient and comprehensive action to be undertaken in the communications sector with the aim of ensuring the security of supply. Efforts would need to be made to minimise overlaps between the different measures.

The measure presented here would accomplish this in regard to the security of supply, thus avoiding unnecessary use of public resources. The committee's collaborative work could also further the search for policy solutions that are of significance for the security of supply and which could be used to better safeguard the functions vital to society in securing the functioning of ICT systems by means other than committing state capital.

It is also important to begin producing information that would allow a detailed analysis particularly of the effects of various ownership policy alternatives, within the framework of the existing ICT market and public-sector bodies.

This proposed measure is expected at most to lead only to a need for technical amendments to the legislation.

8. In implementing the proposals set out above, the national information infrastructure produced by the security network project for the government sector and based on a high level of contingency preparation should be utilised wherever possible. In addition, the requirements set out in the SOPIVA document on contract-based contingency preparations should be introduced throughout the government sector and in companies critical for the security of supply by the end of 2012.

The security network project for the government sector and the project's impacts are discussed elsewhere.

The principal impact of contract-based contingency preparations would arise from the fact that a mechanism would be included in normal ICT system commercial supply and procurement chains with which the system's security would be ensured throughout and at each stage in the chain.

In the invariably changing production networks for information system services, the delivery performance of service production requires that its continuity is systematically managed across the entire service production network, including support services. The security of supply will improve when contingency preparations are included at an early stage in contracts, and when there is a considerable increase in society's awareness of the aims of security of supply.

This proposed measure would not give rise to the need for legislative amendments but it could have financial implications as the quality of production chains is improved.